1 Basics of Quantum Computation

1.1 Qubits [1]

The fundamental unit of quantum information is the qubit. Unlike a classical bit, a qubit can exist in a coherent superposition of its two states, denoted as $|0\rangle$ and $|1\rangle$. These fundamental states are physically realized as charge states in superconducting circuits, the spin of an electron in quantum dots, or atomic spin states. An arbitrary state$|\psi\rangle$ for qubits are expressed as:

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle \tag{1}$$

where $|0\rangle$ and $|1\rangle$ are two orthogonal basis states in hilbert space $\mathcal{H}$ and $|\alpha|^2 + |\beta|^2 = 1$. In the state vector representation, $|0\rangle$ and $|1\rangle$ are commonly expressed as:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{2}$$

Unlike classical processing, quantum gates acting on the Hilbert space of qubits must conserve the probability of the qubit states and are therefore unitary. we can define individual qubit gate I, X, Y and Z called Pauli gate. These gates have the following properties:

$$\begin{aligned}
&I|0\rangle = |0\rangle, \quad I|1\rangle = |1\rangle, \\
&X|0\rangle = |1\rangle, \quad X|1\rangle = |0\rangle, \\
&Y|0\rangle = -i|1\rangle, \quad Y|1\rangle = i|0\rangle, \\
&Z|0\rangle = |0\rangle, \quad Z|1\rangle = -|1\rangle
\end{aligned} \tag{3}$$

where i is the imaginary unit. Thus, I is called the identity matrix and acts on a qubit trivially. From Eq. (3), one can derive the matrix representations of the I, X, Y and Z gates as:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{4}$$

If we have multiple qubits, for example, two qubits with states $|0\rangle$ and $|1\rangle$, we represent their combined state using the Kronecker product symbol $\otimes$ as $|0\rangle \otimes |1\rangle = |01\rangle$. In the same way, if we have n states of $|0\rangle$, we represent these states as $|00\cdots 0\rangle$. For short, we denote it as $|0\rangle^n$. Additionally, we can define mutiple qubits gate G as:

$$G = \bigotimes_{i=1}^{n} P_i = P_1 \otimes P_2 \otimes \cdots \otimes P_n = P_1 P_2 \cdots P_n \tag{5}$$

where P_j is single qubit gate for jth qubit.

1.2 Gates

In Section 1.1, we introduced only the Pauli gates I, X, Y, and Z. The n-qubit Pauli gates are denoted as a group $\mathcal{P}_n$. There exist additional gates, which can be classified as either Clifford or non-Clifford gates. The definitions of Clifford gates and non-Clifford gates are given as follows.

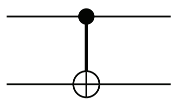
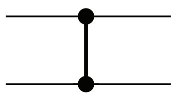
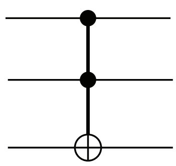
Definition 1. *A group of n-qubit Clifford gates $\mathcal{C}_n$ is defined as:*

$$\mathcal{C}_n = \{V \in U(n) \mid V\mathcal{P}_n V^\dagger \in \mathcal{P}_n\}, \tag{6}$$

where $U(n)$ denotes the n-qubit unitary group. Non-Clifford gates belong to a group disjoint from the Clifford group.

In the context of quantum computing, we often use various Clifford and non-Clifford gates to construct circuits. The circuit diagrams and matrix representations of these gates are shown in Fig. 1. An operator is synonymous with a gate in the context of quantum computing. One can verify that X, Y, Z, H, S, $CNOT$, and CZ are Clifford gates, while T and CCX are non-Clifford gates, as defined in Definition1.

Table 1

Operator	Gate (in a circuit)	Matrix
Pauli-X (X **)**	$-\boxed{\text{X}}-$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
Pauli-Y (Y **)**	$-\boxed{\text{Y}}-$	$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$
Pauli-Z (Z **)**	$-\boxed{\text{Z}}-$	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
Hadamard (H **)**	$-\boxed{\text{H}}-$	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
Phase (S **)**	$-\boxed{\text{S}}-$	$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$
π / 8 (T **)**	$-\boxed{\text{T}}-$	$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$
Controlled Not ($CNOT$, CX **)**		$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$
Controlled Z (CZ **)**		$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$
Toffoli (CCX **)**		$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$

When we use only Clifford gates, we perform only Clifford operations. However, it has been proven that Clifford operations can be efficiently simulated on a classical computer, as stated in the Gottesman-Knill theorem [2]. To achieve quantum supremacy, we must use non-Clifford operations for universal computation. However, such non-Clifford operations are very costly because they cannot be error-corrected in quantum error correction theory. To implement non-Clifford operations, we must perform magic state distillation [3].